DRAFT

X.509 Certificate Policy For The

Federal Bridge Certification Authority (FBCA)

Version 1.0

18 December 1999

DRAFT

1. INTRODUCTION

This document defines four certificate policies for use by the Federal Bridge Certification Authority (FBCA) and Agency CAs, representing four different assurance levels (Rudimentary, Basic, Medium, and High) for public key digital certificates. This Certificate Policy (CP) is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Part˚4 Certificate Policy and Certification Practice Statement Specification.

The FBCA supports interoperability among Federal Agency PKI domains in a peer to peer fashion. The FBCA certificates thus act as a conduit of trust. It does not add to and should not subtract from trust relationships which exist between the transacting parties as established through the Federal PKI Policy Authority (FPKIPA). The FBCA will issue certificates only to those Agency CAs determined by the owning agency (called Principal CAs).

At their discretion, agencies may elect to interoperate among themselves without using the FBCA. Those agencies that elect to do so may nonetheless employ levels of assurance that mimic those set forth in the FBCA CP. However, FBCA CP Object Identifiers (OIDs) may only be used by agencies that interoperate with the FBCA. Any use of or reference to this FBCA CP outside the purview of the FPKIPA is completely at the using parties risk. Further, an Agency shall not assert the FBCA CP OIDs in any certificates the Agency CA issues, except in the policyMappings field establishing an equivalency between an FBCA OID and an OID in the Agency CA s CP.

The terms and provisions of this FBCA CP shall be interpreted under and governed by applicable Federal law. The United States Government disclaims any liability that may arise from the use of this FBCA CP.

1.1 Overview

1.1.1 ***Certificate Policy (CP):*** FBCA certificates contain a registered certificate policy object identifier (OID), which may be used to decide whether a certificate is trusted for a particular purpose. The party that registers the OID (in this case, the U.S. Government) also publishes the CP, for examination by relying parties. Each FBCA certificate must refer to this CP and will also, in the policy mappings extension field and in whatever other fashion is determined by the FBCA OA to be necessary for interoperability, reflect what mappings the FPKIPA determines shall exist between the FBCA CP and the affected Agency CA CP.

1.1.2 ***Relationship Between the FBCA CP and the FBCA CPS:*** The FBCA CP states what assurance can be placed in a cross certificate issued by the FBCA. The FBCA CPS states how the FBCA establishes that assurance.

1.1.3 ***Relationship Between the FBCA CP and the Agency CA CP:*** The levels of assurance of the certificates issued under the FBCA CP are mapped by the FPKIPA to the levels of assurance of the certificates issued by Agency CAs, and that information

(the policy mappings) is placed into the certificates issued by the FBCA, or otherwise published or used by the FBCA OA so as to facilitate interoperability.

1.1.4 ***Interoperation with CAs External to the Federal Government:*** The current version of this CP does not provide for interoperability through the FBCA between Federal Agency PKI domains and those of parties external to the Federal government. Such interoperability will be established when directed by the FPKIPA and will require changes to this CP to address issues associated with liability and other matters. Nonetheless, it is the ultimate intent of the FPKIPA to make the FBCA available to support interoperability between Federal and non-Federal entities. Moreover, interoperability with parties external to the Federal government for purposes of technical testing may be performed when directed, and in a fashion determined by, the FPKIPA.

1.2 Identification

There are four levels of assurance in this policy. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the FBCA. The FBCA OIDs are identified as follows:

id-fpki-certpcy-rudimentaryAssurance	::= id-fpki-certpcy-1
id-fpki-certpcy-basicAssurance	::= id-fpki-certpcy-2
id-fpki-certpcy-mediumAssurance	::= id-fpki-certpcy-3
id-fpki-certpcy-highAssurance	::= id-fpki-certpcy-4

1.3 Community and Applicability

The following are roles relevant to the administration and operation of the FBCA:

1.3.1 ***Federal PKI Policy Authority (FPKIPA)*** — The group of agencies established pursuant to the Government Information Technology Services Board (GITS Board) charter which is responsible for the FBCA CP and CPS, for accepting applications from agencies desiring to interoperate using the FBCA, determining the mappings between certificates issued by applicant Agency Principal CAs and the levels of assurance set forth in the FBCA CP; and after an Agency is authorized to interoperate using the FBCA, ensuring continued conformance of that Agency with applicable requirements as a condition for allowing continued interoperability using the FBCA.

1.3.2 ***FBCA Operational Authority (FBCA OA):*** The organization which operates the FBCA, including issuing certificates when directed by the FPKIPA, posting those certificates and Authority Revocation Lists (ARLs - which are CRLs for CA cross-certificates) into the FBCA directory, and ensuring continued availability of the directory to all users.

1.3.3 ***FBCA Operational Authority Administrator:*** The individual within the Operational Authority who has principal responsibility for overseeing the proper operation of the FBCA including the FBCA directory.

1.3.4 ***FBCA Operational Authority PKI Officers*** — The individuals within the Operational Authority, selected by the Administrator, who operate the FBCA and its directory including executing FPKIPA direction to issue FBCA certificates to Agency Principal CAs or taking other action to effect interoperability between the FBCA and Agency Principal CAs.

1.3.5 ***Agency Principal CA*** — An entity within an Agency which the Agency has determined should interoperate directly with the FBCA (e.g., through the exchange of cross-certificates), and which issues either end-entity certificates to Agency users, or cross-certificates (or other means of interoperation) to other Agency or external party CAs, or both. It should be noted that an Agency may request that the FBCA interoperate with more than one CA within the Agency; that is, an Agency Principal CA need not be unique.

1.3.8 ***Applicability***

1.3.8.1 ***Assurance levels:*** The sensitivity of the information processed or protected using certificates issued by FBCA or an Agency CA will vary significantly. Agencies must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Agency for each application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at four increasing, qualitative levels of assurance: Rudimentary, Basic, Medium and High.

Rudimentary: Provides the lowest level of assurance. This level of assurance is relevant to environments in which the threat of malicious activity is considered to be low. It includes basic security requirements (i.e., audit, archive, and backup and recovery). The Rudimentary level of assurance differs from higher levels in several aspects; for example, all cryptographic functions to be performed by cryptographic modules must be validated only to FIPS 140 Security Level 1. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.

Basic: Provides a basic level of assurance. This level of assurance is relevant to environments where there are risks and consequences of data compromise but they are not significant. It is assumed at this security level that the users are not malicious. This level of assurance requires, at a minimum, two distinct roles. One role will be responsible for account administration, key generation, audit and archive configuration and a second role responsible for issuing and revoking certificates. This level of assurance increases the number of

events that must be audited and requires increased cryptographic protection of audit logs, archives, and system backups. In addition, FIPS 140 Security Level 2 (or higher) cryptographic modules are required for the protection of some private keying material.

Medium: This level of assurance is relevant to environments where risks and consequences of data compromise are moderate. This level of assurance requires additional integrity controls to ensure data is not modified, and provides some protection against malicious authorized users by requiring additional role separation and more than one individual in a role to perform certain functions. The FBCA or Agency CA operating at this assurance level includes protections to protect against someone with physical access to the components and includes additional assurance requirements to ensure the FBCA or Agency CA is functioning securely.

This level of assurance requires, at a minimum, three distinct roles. One role will be responsible for account administration, key generation, and audit and archive configuration; a second role will be responsible for issuing and revoking certificates; and a third role responsible for maintaining the audit logs and archives. This level of assurance requires two-party control of private key export and additional auditing of import and export of secret and private keys and requests for information. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140 Security Level 2 or higher. Finally, there is increased public key protection and digital signatures are required on all messages.

High: This level of assurance may be appropriate for use where the threats to and consequences of data compromise are significant. The environment and the users may be hostile. This level of assurance is intended to protect against malicious authorized and unauthorized users by requiring, at a minimum, four distinct roles. One role will be responsible for account administration and key generation; a second role responsible for maintaining the audit logs and archives; a third role responsible for issuing and revoking certificates; and a fourth role responsible for performing backups. This level of assurance requires significant assurance that the security features are functioning properly, and increases the integrity of audit logs and archives by requiring signed third-party timestamping. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140 Security Level 3 or higher.

2. GENERAL PROVISIONS

2.1 Obligations: The obligations described below pertain to the FBCA, and to Agency Principal or other CAs, which either interoperate with the FBCA or are in a trust chain up to a Principal CA which interoperates with the FBCA. The obligations applying to Agency Principal or other CAs pertain to their activities as issuers of certificates. Further, the obligations focus on Agency CA obligations affecting interoperability with the FBCA. Thus, where the obligations include, for example, a review (or audit) by the FPKIPA or some other body of an Agency s CA operation, the purpose of that review pertains to interoperability using the FBCA, and whether the agency is complying with the Memorandum of Agreement (MOA) it entered into with the FPKIPA to interoperate with the FBCA.

2.1.4 ***Relying Party Obligations:*** The certificates or other digitally signed instruments issued by the FBCA and, where applicable, Agency CAs, will reside in the FBCA X.500 directory. The FBCA directory will be publicly accessible at all times. When a subscriber relying party wishes to determine whether to accept a certificate issued by another Agency s CA for a transaction, the subscriber relying party may use certificates issued by the FBCA to create a trust path of certificates from the domain of its Agency s CA to the domain of the issuing Agency s CA, and then determine whether the issuing Agency s certificate as offered contains sufficient assurance to allow the transaction to consummate. Alternatively, the relying party may employ other digitally signed material provided by the FBCA or Agency CA that fulfills the same functionality as certificates.

The FBCA CP does not determine what steps the subscriber relying party should take to determine whether to allow the transaction to consummate. In other words, it does not compel the relying party to perform X509 path processing, or to determine whether any certificates in the trust path have been revoked. The subscriber relying party decides, on its own accord, what steps to take; the FBCA merely provides the tools needed to perform the trust path creation and certificate policy mappings which the subscriber relying party may wish to employ in its determination.

2.2 ***Financial responsibility:*** This CP contains no limits on the usage of any certificates, issued by the FBCA or by Agency CAs. Rather, agencies, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction. Thus, one agency may be willing to accept a Basic level certificate for transactions of a financial value for which another Agency would require a High level certificate. This is entirely at the discretion of the Agency as relying party and is likely to depend upon several factors in addition to the certificate assurance level (e.g., likelihood of fraud, other procedural controls, agency-specific policy or statutorily imposed constraints, etc.).

2.7 ***Compliance Audit:*** All personnel shall be watchful for attempts to violate the integrity of the FBCA or Agency CA system. The audit log shall be checked for anomalies which may indicate a violation attempt, including repeated failed actions, unauthorized requests for privileged information, unauthorized attempted access of system files, and unauthenticated responses. Auditors shall also check for continuity of the audit log

2.7.1 ***Frequency of Entity Compliance Audit:*** The FPKIPA shall publish requirements governing when and how audits or other reviews will be performed of the FBCA and Agency CAs to ensure continued compliance with the obligations set forth in the MOA which an agency enters into with the FPKIPA to interoperate with the FBCA; such obligations will include compliance with this CP.

2.7.5 ***Actions taken as a result of deficiency:*** The FPKIPA may determine that an Agency is not complying with its obligations set forth in this CP and expressed in the MOA between the FPKIPA and the Agency covering the operation of the Agency CA or Agency RAs. When such a determination is made, the FPKIPA may direct the FBCA OA to cease interoperating with the Agency Principal CA (e.g., by revoking the certificate that the FBCA had issued to the Agency Principal CA). Procedures for this purpose will be published by the FPKIPA.

3. IDENTIFICATION AND AUTHENTICATION

3.1 ***Initial Registration:*** The FBCA or Agency CA must ensure that the applicant s identity information and public key are adequately bound. The FBCA or Agency CA must specify in its respective CPS procedures for authenticating a subscriber's identity in accordance with the requirements of this CP. Additionally, the FBCA or Agency CA must record the process that was followed for issuance of each certificate. Depending upon the certificate level of assurance, process documentation may include the identity of the person performing the identification, a signed declaration by that person that they verified the identity of the subscriber against an official government-issued photo ID, an identifying number of the ID, and the date and time of the verification. Additionally, where appropriate, the process documentation should include a declaration of identity signed with a handwritten signature, by the certificate applicant in the presence of the person performing the identity authentication

Assurance Level	**Identification**
Rudimentary	E-mail addresss
Basic	No specific need required Identity may be established by database, supervisor, or subscriber
Medium	Need must be identified Must appear in person to a Registration Authority or designated representative and present appropriate proof of identity (may include picture ID)
High	Need must be identified Must appear in person to a Registration Authority or designated representative, and present appropriate proof of identity (including official picture ID)

3.1.1 *Assurance Levels:*

3.1.1.1 ***Rudimentary:*** The applicant may apply through an open network (such as the Internet), and need only present rudimentary information, such as an e-mail address. The private key corresponding to the public key offered for the certificate may exist in any software or hardware form. The certificate shall contain either a non-null Subject Name or, if a null Subject Name, it shall contain an Alternative Subject Name that is populated and marked critical. This level is intended only for ensuring data integrity checking. It is not suitable for authentication or digital signatures. Additionally, this level may be used to achieve modest confidentiality but only if certificates at higher levels of assurance are not available.

3.1.1.2 ***Basic:*** The applicant may apply in person or through a network (such as the Internet), but if the latter is used, the connections between the applicant and the Registration Authority or its designated representative (for registration) and Certification Authority (for transport of the public key for certificate issuance) shall be secured using a protocol approved by the FPKIPA that provides for strong encryption of the transferred information. The applicant must supply sufficient information to uniquely identify the applicant, and the RA must vet the information to confirm identity. The private key corresponding to the public key offered for the certificate may exist in software or a hardware token, and its possession by the applicant must be proven in accordance with PKIX Certificate Management Protocol or an equivalent protocol approved by the FPKIPA. The certificate shall contain a non-null Subject Name, and may contain an Alternative Subject Name marked as non-critical.

3.1.1.3 ***Medium:*** Same as Basic except that the applicant must appear in person before a Registration Authority or its designated representative, and the certificate shall contain a Distinguished Name and may contain an Alternative Subject Name marked as non-critical.

3.1.1.4 ***High:*** Same as Medium, except that the applicant must present at least two forms of government issued identification (at least one of which shall be a picture identification such as a drivers license or passport). The subscriber s identity shall be personally verified by a Registration Authority or designated representative prior to the subscriber s certificate being enabled. There are two ways to meet this requirement:

- The subscriber shall personally appear before the Registration Authority or designated representative at any time prior to application of the CA s signature to the applicant s certificate, or

- When private keys are delivered to subscribers via hardware tokens, the subscribers shall personally appear before the Registration Authority or designated representative to obtain their tokens or token activation data.

Minors and others not competent to perform face-to-face registration alone shall be accompanied by a person already issued a digital certificate by the Agency, and who will present information sufficient for registration at the level of the certificate being requested, for both himself and the person accompanied.

3.1.2 ***Mapping Agency Subscriber Certifications to FBCA CP Levels of Assurance:*** For an Agency to obtain an FBCA certificate (or equivalent) for a Principal CA within that Agency, the Agency must meet the Agency s own certification requirements and the requirements of this CP. This paragraph applies to certificates issued by Agency CAs to their subscribers. The requirements in this paragraph will be used by the FPKIPA to determine the mappings between the levels of assurance expressed in the Agency CA s CP, and those in the FBCA CP, set forth below for each level of assurance in the FBCA CP.

3.2 ***Types of names:*** The FBCA (and where required, Agency CAs) shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN). Certificates issued to Agency CAs and RAs shall use the DN form, and have an assurance level equal to, or greater than, the highest level of assurance of the certificates the CA issues to subscribers or other CAs. Where DNs are required, subscribers will have them assigned through their organizations, in accordance with a naming authority. Certificates may additionally assert an alternate name form, where allowed.

Rudimentary	Non-Null Subject Name, or Null Subject Name if Alternative Subject Name is populated and marked critical
Basic	Non-Null Subject Name, and Alternative Subject Name marked non-critical
Medium	X.500 Distinguished Name, and Alternative Subject Name marked non-critical
High	X.500 Distinguished Name, and Alternative Subject Name marked non-critical

3.3 ***Need for names to be meaningful:*** Names used shall identify the person or object to which they are assigned in a meaningful way. The CA which issues the certificate shall ensure that an affiliation exists between the subscriber and any organization that is identified by any component of any name in its certificate. When DNs are used, the common name shall represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For

equipment, this may be a model name and serial number, or an application process (e.g., *Organization X Mail List* or *Organization Y Multifunction Interpreter*). The FPKIPA will ensure DNs are used in certificates issued by the FBCA. In the case where one Agency CA certifies another, the certifying Agency CA must impose restrictions on the name space authorized in the subordinate Agency CA which are at least as restrictive as its own name constraints. When technical means exist for imposing these constraints (such as the name constraints certificate extension), they shall be used. Otherwise, these constraints shall be imposed procedurally or by policy.

3.4 ***Rules for interpreting various name forms:*** Rules for interpreting name forms are contained in the applicable certificate profile established by the FPKIPA or Agency CA.

3.5 ***Uniqueness of names:*** Through the MOA which the FPKIPA executes with an Agency prior to allowing interoperation between the FBCA and an Agency Principal CA, the FPKIPA shall ensure that appropriate control over the name space is executed to preclude ambiguity or confusion.

4. OPERATIONAL REQUIREMENTS

4.1 ***Application by an Agency for an FBCA Certificate:*** This paragraph applies to agencies seeking FBCA certificates for their Principal CAs. The FPKIPA will establish and publish (separate from this FBCA CP) procedures for agencies to use in applying for a certificate from the FBCA. The FPKIPA will act on the application, and upon making a determination to issue a certificate and entering into an appropriate interagency agreement with the applicant Agency which sets forth respective responsibilities, will instruct the FBCA Operational Authority to issue the certificate to the applicant Agency. The applicant Agency Principal CA shall have a clearly distinguishable and unique distinguished name as defined in X509, and that shall be placed in the certificate subject name field. The names asserted in the FBCA issued certificates shall be the official names of the Agency affiliated with the cross-certified CA, or an officially recognized acronym (such as FBI, DOJ, and others.).

4.2 ***Certificate issuance:***

4.2.1 ***FBCA and Agency Principal CA Certificate Duration:*** The following table summarizes the validity period of a certificate issued by the FBCA to an Agency Principal CA, and the lifetime of the associated Principal CA signing key (used for signing certificates issued to subscribers including other Agency CAs). Signature keys that have expired for the purposes of certificate signature may still be used for ARL signature. All values are in years. The FPKIPA may determine that certificate revocation will be done sooner than planned if the security of the cryptography becomes unacceptably weak.

Assurance Level	FBCA	Agency CA

Rudimentary	10 Years	10 Years
Basic	10 Years	10 Years
Medium	10 Years	10 Years
High	10 Years	10 Years

4.4 Certificate Suspension and Revocation

4.4.1 ***Revocation of a Certificate Issued by the FBCA:*** Revocation will be accomplished by the immediate generation and publication into the FBCA directory of an Authority Revocation List (ARL) that cites the certificate as revoked, identifies the certificate being revoked and the reason for the revocation. Further, and separate from the publication of the ARL, prompt oral or electronic notification will be given by the FBCA OA to previously designated officials in all agencies having a Principal CA with which the FBCA interoperates.

4.4.2 ***Revocation of a Certificate Issued by an Agency Principal CA:*** Revocation shall be effected by the publication of a CRL (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) within the time limits specified below (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). Certificates that are revoked shall remain on the CRL until they expire. The certificates may be removed from the second CRL issued after they expire.

Assurance Level	**CA Revocation**
Rudimentary	Not Required
Basic	Within 6 hours
Medium	Within 2 hours
High	Within 30 Mins

4.4.3 ***Circumstances for revocation:*** Where revocation is required as described below, it shall be done when an Agency principal CA receives sufficient evidence of compromise or loss of the corresponding private key, or when an authenticated request is made to the Agency principal CA by the holder of the private key or someone in his or her supervisory chain.

4.4.5 ***Who can request revocation:*** A certificate may be revoked upon direction of the Federal Public Key Infrastructure Policy Authority (FPKIPA) or upon an authenticated request by a previously designated official of the Agency responsible for the Principal CA (such official or officials shall be identified in the interagency agreement between the FPKIPA and the Agency as authorized to make such a request). The FPKIPA shall establish and publish (separate from this FBCA CP) the process which it will use to determine whether a certificate issued to an Agency Principal CA shall be revoked in the absence of an authenticated request.

4.4.12 ***ARL/CRL Issuance Frequency:*** ARL/CRLs will be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Each ARL/CRL has a duration which is composed of two data fields; date of issue and date of next issue . Each ARL/CRL shall be published before the date of next issue of the previous ARL/CRL published. This will facilitate the local caching of ARL/CRLs for off-line or remote (laptop) operation. Agencies shall coordinate with the repositories to which they post ARL/CRLs to reduce latency between creation and availability. Superceded ARL/CRLs shall be removed from the directory system upon posting of the latest ARL or CRL.

The FBCA shall publish an ARL at least once per week, with a duration of no more than two weeks. An ARL shall be published immediately in the event of an Agency principal CA private key compromise or loss.

Agency principal CAs should routinely publish revocation information for each level of assurance as set forth below, and promptly in the event of a subscriber private key compromise or loss:

Assurance Level	**Minimum Publication Frequency (other than for loss or compromise of private key)**	**Duration**
Rudimentary	Not Required	Not Required
Basic	Once Per Week	<= 2 Weeks
Medium	Once Per Day	<= 2 Days
High	Once Every 12 Hours	<= 1 Day

4.4.13 ***On-line Revocation / Status checking availability:*** CAs and relying party client applications may optionally support On-line revocation/status checking. If a relying party will be operating in an environment where On-line revocation/status checking is not possible, then the CAs shall be required to support CRLs. Clients using On-line revocation/status checking need not obtain or process CRLs.

4.5 ***Security Audit Procedure:*** Audit log files will be generated for all events relating to the security of the FBCA or Agency CAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a log book, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section will be created and maintained.

4.5.1 ***Types of Events Recorded:*** All security auditing capabilities of the FBCA or Agency CA Operating System and PKI CA applications shall be enabled. As a result, most of the events identified in the table below will be automatically recorded. At a

minimum, each audit record shall include the following (either recorded automatically or manually for each type of event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the FBCA or Agency CAs signing process
- A success or failure indictor when performing certificate revocation
- Identity of the entity and/or operator (of the FBCA or Agency CA) that caused the event.
- Messages from any source requesting an action by the FBCA or Agency CA. The messages must include message source, destination and contents.

Auditable Event	Rudimentary	Basic	Medium	High
SYSTEM EVENTS				
Installation of the Operating System	X	X	X	X
Installation of the FBCA or Agency CA	X	X	X	X
Installing hardware cryptographic modules			X	X
Removing hardware cryptographic modules			X	X
Destruction of cryptographic modules	X	X	X	X
System Startup	X	X	X	X
Logon Attempts to FBCA or Agency CA Apps		X	X	X
Receipt of Hardware / Software			X	X
Configuration changes to the server involving:			X	X
Hardware		X	X	X
Software		X	X	X
Operating System		X	X	X
Patches		X	X	X
Users			X	X
Security Profiles			X	X
Administrator privileges		X	X	X
Auditing (frequency, parameters, event type)	X	X	X	X
PHYSICAL ACCESS				
Personnel Access to room housing FBCA or Agency CA			X	X
Access to the FBCA or Agency CA server			X	X
Known or suspected violations of physical security			X	X
UNEXPECTED ANOMALIES				
Error conditions		X	X	X
Software check integrity failures		X	X	X
Receipt of improper messages			X	X
Misrouted messages			X	X
Network attacks (both suspected and confirmed)	X	X	X	X
Equipment failure			X	X

Power outages			X	X
UPS cycling			X	X
Network failures			X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certificate Practice Statement	X	X	X	X
Resetting Operating System clock		X	X	X
Modifications of Audit Logs	X	X	X	X
FBCA OR AGENCY CA OPERATOR ACTIONS				
Account management		X	X	X
Creation of FBCA or Agency CA Users	X	X	X	X
Deletion of FBCA or Agency CA Users	X	X	X	X
Attempts to set passwords		X	X	X
Attempts to modify passwords		X	X	X
Backing up FBCA or Agency CA database		X	X	X
Restoring FBCA or Agency CA database		X	X	X
File manipulation			X	X
Posting of any material to a repository			X	X
Access to FBCA or Agency CA database			X	X
Any use of the FBCA or Agency CA signing key	X	X	X	X
Messages received from any source requesting:				
Certificate requests		X	X	X
Certificate signing		X	X	X
Certificate Revocation		X	X	X
Compromise notification		X	X	X
Actions taken in response to requests from any source				
Certificate issuance	X	X	X	X
Certificate Revocation		X	X	X
Loading tokens with certificates			X	X
Shipment of Tokens			X	X
Zeroizing tokens		X	X	X

4.5.2 ***Frequency of processing log:*** Audit logs shall be reviewed in accordance to the table below. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews must be documented.

Assurance Level	**Review Audit Log**
Rudimentary	Once Per Month
Basic	Once Per Week
Medium	Once Per Week

High	Once Per Week

4.5.3 ***Retention period for audit log:*** Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the FBCA or Agency CA system shall be an official different from the individuals who, in combination, command the FBCA or an Agency CA signing key.

4.5.4 ***Protection of audit log:*** The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, or deletion. FBCA or Agency CA system configuration and procedures must be implemented to ensure that only authorized personnel can archive and view the audit logs. Procedures must be implemented to protect the logs from deletion or destruction prior to the end of the security audit log retention period. The security audit logs (or official copies thereof) must be maintained at a safe and secure storage location separate from the FBCA or Agency CA.

4.5.5 ***Audit log backup procedures:*** Audit logs and audit summaries must be backed up at least monthly. A copy of the audit log will be sent off-site in accordance with the CPS on a monthly basis.

4.5.6 ***Audit collection system (internal vs. external):*** The audit log collection system need not be external to the FBCA or Agency CA system. The audit process shall not be done by or under the control of the FBCA OA (or comparable authority for an Agency CA). Audit processes will be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the FBCA OA Administrator (or comparable Agency authority) shall determine whether to suspend FBCA (or Agency CA respectively) operation until the problem is remedied.

4.5.7 ***Notification to event-causing subject:*** This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

4.6 Records Archival

4.6.1 ***Types of data archived:*** FBCA or Agency CA archive records shall be detailed enough to establish the proper operation of the FBCA or Agency CA, or the validity of any certificate (including those revoked or expired) issued by the FBCA or Agency CA.

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

Data To Be Archived	Rudimentary	Basic	Medium	High

FBCA or Agency CA accreditation (if applicable)	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
All ARLs and CRLs issued and/or published		X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents		X	X	X
Documentation required by compliance auditors		X	X	X

4.6.2 ***Retention period for archive:*** Archive records shall be kept for a period to be determined by the FPKIPA (or Agency CA s governing body) to ensure the ability to confirm the validity of any trust path employing an FBCA (or Agency CA respectively) certificate. The minimum retention period for archive data is as follows:

Assurance Level	**Retention Period**
Rudimentary	7 Years & 6 Months
Basic	10 Years & 6 Months
Medium	20 Years & 6 Months
High	20 Years & 6 Months

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for as long as necessary as determined by the FPKIPA for the FBCA (or Agency CA governing body for the Agency CA).

4.6.3 ***Protection of archive:*** No unauthorized user shall be permitted to write to, modify, or delete the archive. For the FBCA, archived records may be moved to another medium when authorized by the FBCA OA Administrator. The contents of the archive shall not be released except as determined by the FPKIPA for the FBCA (or Agency CA governing body for the Agency CA) or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in at least two safe, secure storage facilities separate from the FBCA or Agency CA itself.

4.6.4 ***Archive backup procedures:*** Archive records shall be labeled at a minimum with the FBCA's or Agency CA s distinguished name, the date, and other identifying data.

4.6.7 ***Procedures to obtain and verify archive information:*** Procedures detailing how to create, package, transmit, and store the archive information shall be published in the FBCA or Agency CA CPS.

4.8 Compromise and Disaster Recovery

4.8.1 ***Computing resources, software, and/or data are corrupted:*** If FBCA or Agency CA equipment is damaged or rendered inoperative, but the FBCA or Agency CA signing keys are not destroyed, FBCA or Agency CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate ARLs/CRLs.

4.8.2 ***FBCA or Agency CA signing keys are revoked:*** If the FBCA or Agency CA cannot reestablish revocation capabilities within the time periods specified above, then the FBCA or Agency CA must report certificates as revoked with a reason code of cessation of operations, and reestablish operation in accordance with procedures set forth in the respective CPS. In the case of a disaster where the FBCA or Agency CA installation is physically damaged and all copies of the FBCA or Agency CA signing keys are destroyed as a result, then the FBCA or Agency CA shall promptly and securely advise all agencies to which it has issued certificates and request that the agencies revoke the cross-certificates they have issued to the FBCA or Agency CA.

4.8.3 ***FBCA or Agency CA signing keys are compromised:*** If the FBCA or Agency CA signing keys are compromised or lost (such that compromise is possible but not certain), all members of the FPKIPA shall be immediately notified (so that agencies may issue ARLs revoking any cross-certificates issued to the FBCA), an ARL shall be immediately published as set forth above, a new FBCA or Agency CA key pair shall be generated by the FBCA or Agency CA in accordance with procedures set forth in the FBCA or Agency CA CPS, and new FBCA or Agency CA certificates issued to agencies also in accordance with the FBCA or Agency CA CPS. The FBCA OA or Agency CA governing body shall also investigate and report to the FPKIPA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

4.9 ***FBCA Termination:*** FBCA termination will occur upon direction of the FPKIPA or dissolution of the MOA between the FPKIPA and FBCA OA, and shall be executed in accordance with procedures set forth in the FBCA CPS.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 *Physical Controls for the FBCA or Agency CA*

5.1.1 ***Site location and construction:*** The location and construction of the facility housing FBCA equipment shall be consistent with facilities used to house high value sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the FBCA equipment and records.

5.1.2 ***Physical access:*** Since the FBCA must plan to issue certificates at all levels of assurance, it must be operated and controlled on the presumption that it will be issuing at least one High assurance certificate. Thus, the FBCA site shall satisfy the requirements for a high security zone, be manually or electronically monitored for unauthorized intrusion at all times, ensure no unescorted access to the FBCA server is permitted, ensure a site access log is maintained and inspected periodically, and ensure all removable media and paper containing sensitive plaintext information are stored in secure containers.

5.1.3 ***Power and air conditioning:*** The facility which houses the FBCA shall be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility must be supplied with sufficient utilities to satisfy operational, health, and safety needs. The FBCA shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The FBCA directory (containing FBCA issued certificates and ARLs) shall be provided with Uninterruptable Power Supplies and backup power generation sufficient for a minimum of 48 hours operation in the absence of commercial power, to support FBCA operation and smooth shutdown if necessary.

5.1.4 ***Water exposures:*** FBCA equipment shall be installed such that it is not in danger of exposure to water, e.g., on tables or elevated floors. Moisture detectors shall be installed in areas susceptible to flooding.

5.1.5 ***Fire prevention and protection:*** An automatic fire (smoke) detection system, and fire extinguishing equipment, shall be installed.

5.1.6 ***Media storage:*** Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the FBCA.

5.1.7 ***Waste disposal:*** Normal office waste shall be removed or destroyed in accordance with applicable policy. Media used to collect or transmit sensitive information (as determined by the FPKIPA) shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 ***Off-site backup:*** At least two backup copies of any information required to restore FBCA operation or respond to requests for archival information shall be stored at an offsite location (separate from the FBCA). The backup shall be stored at a site with physical and procedural controls no less stringent than those of the FBCA. However, no copy of the FBCA private signing key shall be made under any circumstances.

5.2 *Procedural Controls for the FBCA or Agency CA*

5.2.1 ***Trusted Roles:*** A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible and above reproach. The functions performed in these roles form the basis of trust for all uses of the FBCA or an Agency CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The only trusted roles explicitly defined by this CP are the FBCA OA PKI Officer, FBCA System Administrator and FBCA Security Officer. Agency CAs have personnel assigned to analogous roles. For the FBCA, the trusted roles shall be performed as follows (analogous roles for Agency CAs shall be performed in the same fashion):

5.2.1.1 ***FBCA OA PKI Officer:*** Actions taken by the FBCA shall be done under the control of one or more FBCA OA PKI Officers. The FBCA OA Officers must be individually identified by name, and must be present during compliance audits. The FBCA OA PKI Officer(s) role and the corresponding procedures shall be defined in detail in the FBCA CPS. The primary responsibilities include:

- Creation, renewal and revocation of FBCA-issued certificate (requires at least two FBCA OA PKI Officers)
- Posting certificates and ARL|s (requires at least two FBCA OA PKI Officers)
- Performing database backups
- Performing administrative functions such as compromise reporting and maintaining the database
- Programming and managing hardware cryptographic modules (requires at least two FBCA OA PKI Officers)

5.2.1.2 ***Registration Authority (RA):*** The role of the RA is set forth in a CA s CP and CPS. The primary responsibilities of the RA include:

- Verifying identities of Agency principal CAs, either through personal contact, or via agents or employees, in accordance with the FBCA CP and CPS
- Entering subscriber information into the registration system and verifying its accuracy
- Securely communicating registration requests and responses with the FBCA
- Receiving and distributing subscriber certificates

5.2.1.3 ***FBCA System Administrator:*** The FBCA CPS shall define all of the trusted roles for the System Administrator for proper, safe and secure operation of the FBCA equipment and procedures. The responsibilities include:

- Initial configuration of the FBCA, including the installation of the applications, initial setup of accounts, configuration of initial host and network interface

- Creating devices to support recovery from catastrophic system loss
- Performing system backups, software upgrades and recovery
- Modifying host and/or network interface configuration

5.2.1.4 ***FBCA Security Officer:*** The FBCA CPS shall define the responsibilities of the Security Officer to ensure the secure operation of the FBCA equipment and procedures. The responsibilities include:

- Performing or overseeing the performance of compliance audit
- Performing secure storage and distribution of backups and upgrades to an offsite location
- Assigning security privileges and access control of users
- Performing archive and deletion functions of the audit logs
- Reviewing audit logs (requires two FBCA Security Officers)

5.3 *Personnel Controls*

5.3.1 ***Background, qualifications, experience, and security clearance requirements:*** Persons should be selected on the basis of loyalty, trustworthiness, and integrity, and must be US citizens. The FBCA OA Administrator and PKI Officers shall hold Top Secret security clearances; this is necessary even though the FBCA supports transactions only involving unclassified information, because the Administrator and PKI Officers may need to be apprised of potential threat or intelligence information which is classified. Agency CA personnel shall hold security clearances as determined appropriate by their respective Agency.

5.3.3 ***Training requirements:*** All personnel performing duties with respect to the operation of the FBCA or Agency CA must receive comprehensive training. A training plan which includes requirements for refresher training shall be established. Documentation will be maintained identifying all personnel that received training and the level of training completed. Training will be conducted in the following areas:

- CA/RA security principles and mechanisms
- All PKI software versions in use on the CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures.

5.3.8 ***Documentation supplied to personnel:*** The FBCA and Agency CA must make available to its CA and RA personnel the certificate policies it supports, its CPS, and any relevant statutes, policies or contracts.

6. TECHNICAL SECURITY CONTROLS

6.1 *Key Pair Generation and Installation*

6.1.1 ***CA Signing key pair generation:*** All signing key material for certificates issued by the FBCA or Agency CAs shall be generated in hardware modules certified to FIPS 140. For the FBCA, the modules shall meet at a minimum Security Level 3. For Agency CAs, the modules shall meet at a minimum Security Level 1 (for Rudimentary), Security Level 2 (for Basic or Medium), or Security Level 3 (for High).

The private signing key corresponding to the public key offered for the certificate shall have been generated on a hardware token and shall remain only on the token (no copies may be made). The private decryption key corresponding to the public encryption key shall reside on a hardware token but, at the discretion of the Agency, a copy may be made for data recovery purposes. The certificate shall contain a Distinguished Name.

6.1.2 ***FBCA certificates and public key availability and delivery to Principal CAs:*** The FBCA will post the certificates it issues in the FBCA directory. An Agency Principal CA is encouraged to issue certificates to the FBCA directory concurrent with the issuance of an FBCA certificate to the Agency Principal CA. A copy of the FBCA public key will then be available in an Agency Principal CA certificate, which facilitates trust path validation. If an Agency Principal CA elects to issue cross-certificates to the FBCA , then the FBCA shall transport its public key to the Agency Principal CA in a secure, out-of-band fashion to effect certificate issuance.

6.1.5 ***Key sizes:*** The FPKIPA shall determine the appropriate key lengths and corresponding lifetime for each policy level. All FIPS-approved signature algorithms shall be considered acceptable. The current approved key sizes and lifetimes shall be published by the FPKIPA. If the FPKIPA determines that the security of a particular algorithm may be compromised, it may require the FBCA and Agency CAs to revoke the affected certificates.

All certificates issued by the FBCA shall use at least 1024 bit RSA or DSA with Secure Hash Algorithm version 1 (SHA-1) or better in accordance with FIPS 186. Certificates issued by Agency CAs shall use at least 1024 bit RSA or DSA with SHA-1 (or better) in accordance with FIPS 186. Use of SSL or another protocol providing similar security shall require at a minimum triple-DES or equivalent for the symmetric key, and 1024 bit RSA or equivalent for the asymmetric keys.

6.1.6 ***Public key parameters generation:*** Public key parameters for DSA prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

6.1.7 ***Parameter quality checking:*** Pseudo-random numbers for DSA parameters shall be tested as specified in FIPS 186.

6.1.8 ***Hardware/Software key generation:*** Software or hardware may be used to generate pseudo-random numbers, key pairs and symmetric keys. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

The chart below identifies the minimum requirements for using either software or hardware tokens to generate keys in accordance with the appropriate assurance level.

Assurance Level	Key Generation Mechanism
Rudimentary	Software or Hardware
Basic	Software or Hardware
Medium	Software or Hardware
High	Hardware only

6.1.9 ***Key usage purposes (as per X.509 v3 key usage field):*** Since the FBCA s primary role is supporting interoperability among Federal agencies, FBCA certificates will utilize two key usage bits: *ARLSign* and key *CertSign*. There are no other FBCA stipulations.

6.2 *Private Key Protection*

6.2.1 ***Standards for cryptographic module:*** Cryptomodules shall be certified as meeting the FIPS 140 level indicated, or otherwise verified to an equivalent level of functionality and assurance approved by the FPKIPA. All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plain text. No private keys shall appear unencrypted external to the FBCA or Agency CA. No one should have access to a private signing key but the subject of the corresponding certificate.

6.2.2 ***CA private key multi-person control:*** The FBCA or Agency CA private signing key shall be split such that its use will require the cooperation of at least two PKI Officers.

6.2.3 *Key Escrow*

6.2.3.1 ***Escrow of FBCA private signing key:*** Under no circumstances shall the FBCA or an Agency CA signing key be escrowed.

6.2.3.2 ***Escrow of Agency CA encryption keys:*** The FBCA will not perform any encryption key recovery function involving encryption keys issued to Agency CAs, and will not store any information encrypted in the FBCA public key which may require key recovery capabilities. However, if encryption key pairs need to be issued by the FBCA covering directory system access or for other purposes, the FPKIPA shall publish applicable requirements for that purpose.

6.2.4 Private Key Backup

6.2.4.1 ***Backup of FBCA private signing key:*** The FBCA and Agency CA private signing keys may be backed-up under the same multi-person control as the original signing key. Such backup may only create a single copy of the signing key.

6.2.4.2 ***Backup of subscriber private signing key:*** Subscriber private signing keys shall not be backed-up, escrowed, or copied.

6.2.5 ***Private key entry into cryptographic module:*** FBCA and Agency CA private keys are to be generated by and remain in a cryptographic module.

6.2.7 ***Method of activating subscriber private keys:*** Pass-phrases or PINs may be used as a means of user authentication to activate the private key in a cryptomodule. Other methods, such as biometric data, are also acceptable, but not required. Entry of activation data must be protected from disclosure (e.g., the data should not be displayed while it is entered).

6.2.8 ***Methods of deactivating subscriber private keys:*** Cryptomodules which have been activated must not be left unattended or otherwise available to unauthorized access. After use, they must be deactivated. When keys are deactivated they must be cleared from system memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module must automatically deactivate the private key after a period of inactivity determined in the applicable CP. Hardware cryptomodules should be removed and stored in a secure container when not in use.

6.2.9 ***Method of destroying subscriber private keys:*** Private keys must be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. The specific mechanism for destroying subscriber private keys (both hardware and software) will be defined in the applicable CA or CPS.

6.3 Other Aspects of Key-Pair Management

6.3.3 ***Logic for utilizing separate key-pairs for Signature and Confidentiality:*** It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this CP prohibits that condition. Rather, one key-pair shall be used for digital signature, and a separate key-pair shall be used for confidentiality.

A subscriber s key-pair that is used for digital signatures should never be escrowed, archived or backed up. The reason for this is simple: a subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the subscriber must use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or

destroyed, or if the subscriber departs the agency without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, an agency must escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs must be employed.

6.4 Activation Data

6.4.1 ***Activation data generation and installation:*** The activation data used to unlock FBCA, Agency CA or subscriber private keys, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. FBCA, Agency CAs, and subscribers must have the capability to generate new activation data at any time. For Rudimentary, Basic, and Medium, activation data may be user selected. For High, it must either entail the use of biometric data or be randomly and automatically generated. Activation data shall be generated in conformance with FIPS-112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptomodule.

6.4.2 ***Activation data protection:*** Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data either should be biometric in nature or should be memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptomodule is used to protect, and shall not be stored with the cryptomodule. The protection mechanism should include a facility to temporarily lock the account after a predetermined number of login attempts as set forth in the respective CP or CPS.

6.5 *Computer Security Controls*[F1]

6.5.1 ***Specific computer security technical requirements:*** The FBCA and its ancillary parts must include the following functionality: access control to FBCA services and PKI roles; enforced separation of duties for PKI roles; identification and authentication of PKI roles and associated identities; object re-use or separation for FBCA random access memory; use of cryptography for session communication and database security; archival of FBCA history and audit data; audit of security related events; self-test of security related FBCA services; trusted path for identification of PKI roles and associated identities; recovery mechanisms for keys and the FBCA system; enforcement of domain integrity boundaries for security critical processes. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

6.5.2 ***Computer security rating:*** The FPKIPA shall prescribe requirements governing the application of Common Criteria requirements to the FBCA.

6.6 Life-Cycle Technical Controls

6.6.1 ***System development controls:*** The FBCA or Agency CA must use software that has been designed and developed under a development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), or equivalent as determined by the FPKIPA for the FBCA (or comparable Agency CA governing authority for the Agency CA). The design and development process must provide sufficient documentation to support third party security evaluation of the FBCA or Agency CA components.

6.6.2 ***Security management controls*****:** The configuration of the FBCA or Agency CA system as well as any modifications and upgrades must be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the FBCA or Agency CA software or configuration. A formal configuration management methodology must be used for installation and ongoing maintenance of the FBCA or Agency CA system. The FBCA or Agency CA software, when first loaded, must be verified as being identical to that supplied from the vendor, with no modifications, and be the version intended for use. For the FBCA, the integrity of the software shall be verified by the FBCA OA at least weekly (e.g., in conjunction with ARL publication).

6.7 Network Security Controls

The FBCA shall not be connected to any network; the FBCA directory shall be connected to the internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). The FBCA directory and Agency CA equipment may operate through a network guard insofar as the function of the guard is not circumvented. Use of appropriate boundary controls shall be employed to protect FBCA directory or Agency CA equipment against known network attacks. Unused network ports and services shall be turned off. Any network software present on the FBCA directory or Agency CA equipment shall be necessary to the functioning of the FBCA directory or Agency CA application. The FBCA or Agency CA CPS will define the network protocols and mechanisms required for the operation of the FBCA directory or Agency CA.

7. CERTIFICATE AND ARL PROFILES

7.1 Certificate Profile

7.1.1 ***Version number:*** The FBCA and Agency CAs will issue X.509v3 certificates (populate version field with integer "2").

7.1.3 ***Algorithm object identifiers:*** Certificates issued under this CP will use the following OIDs for signatures:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
Id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithm(1) 22}

7.1.4 ***Name forms:*** Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name as specified in [FPKI-E], with the attribute type as further constrained by [RFC2459].

7.1.5 ***Name constraints:*** When used, the name constraints extension shall be populated and processed as described in [FPKI-E].

7.1.6 ***Certificate policy object identifier:*** Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued.

7.2 ARL Profile

7.2.1 ***Version numbers:*** The FBCA will issue X.509 version two (2) ARLs. Agency CAs will also issue X509 version two (2) CRLs.

7.2.2 ***ARL and ARL entry extensions:*** The CPS will define the use of any extensions.

8. SPECIFICATION ADMINISTRATION

8.3 ***Certification Practice Statement:*** The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It will be more detailed than the corresponding certificate policy described in section 2.1 above. The FBCA CPS, which is contained in a separate document published by the FBCA Operational Authority and approved by the FPKIPA, specifies how this FBCA CP is implemented to ensure compliance with its provisions by the FBCA Operational Authority.

9. BIBLIOGRAPHY

The following documents contain information which provide background, examples, or details about the contents of this policy:

ABADSG *Digital Signature Guidelines,* 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.

FOIACT 5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html

PKCS#12 *Personal Information Exchange Syntax Standard*, April 1997. http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

NAG69C *Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C,* November 1999.

NSD42 *National Policy for the Security of National Security Telecom and Information Systems*, 5 Jul 90.
http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft
Digital Signatures, W. Ford
United States Department of Defense X.509 Certificate Policy, Version 4.0, 29 October 1999

10. ACRONYMS AND ABBREVIATIONS

ARL Authority Revocation List
CA Certification Authority
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
CSOR Computer Security Object Registry
DN Distinguished Name
DSA Digital Signature Algorithm
DSS Digital Signature Standard
ERC Enhanced Reliability Check
FAR Federal Acquisition Regulations
FBCA Federal Bridge Certification Authority
FBCA OA Federal Bridge Certification Authority Operating Authority
FED-STD Federal Standard
FIPS PUB (US) Federal Information Processing Standard Publication
FPKISC Federal PKI Steering Committee
FPKIPA Federal PKI Policy Authority
GITSB Government Information Technology Services Board
GPEA Government Paperwork Elimination Act of 1998
IETF Internet Engineering Task Force
ISO International Standards Organization
ITU International Telecommunications Union
ITU-T International Telecommunications Union — Telecommunications Sector
ITU-TSS International Telecommunications Union — Telecommunications System Sector
MOA Memorandum of Understanding
NIST National Institute of Standards and Technology
NSA National Security Agency

OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

11. DEFINITIONS

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.

Attribute Authority	An entity, recognized by the FPKIPA or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authority Revocation List (ARL)	A list of revoked CA certificates. An ARL is a CRL for CA cross-certificates.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this Policy, the term Certificate refers to certificates that expressly reference the OID of this policy in the Certificate Policies field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and ARLs or CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certification Authority Software	The cryptographic software required to manage the certificates of end entities.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions[F2] performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Policy, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine: (1) whether the transformation was created using the key that corresponds to the signer s key; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; date of issue and date of next issue .
Employee	Any person employed by an Agency as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers who are not authorized to issue certificates.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Principal Agency Certification Authorities.

FBCA Operational Authority (FBCA OA)	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure

	communication.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement	Agreement between the FPKIPA and an Agency allowing interoperability between the Agency Principal CA and the FBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each

	of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Positive Control Material	
Principal CA	The Principal CA is one or more Agency CAs that the Agency has selected to interoperate with the FBCA.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law and agency policy.
Private Key	(1) The signing key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The signing key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Rekey (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does

	not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical Non-Repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a security service for legal non-repudiation.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing subscriber identification during the registration process. Trusted agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure, authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]

Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

13. ACKNOWLEDGEMENTS

While a large number of people participated in the development of this Certificate Policy, special thanks are due to the individuals listed below:

Peter Alterman	NIH	Alterma@od1em1.nih.gov
Roger Bezdek	Treasury	Roger.Bezdek@do.treas.gov
Michelle Borzillo	FDIC	mborzillo@fdic.gov
Bill Burr	NIST	william.burr@nist.gov
Dave Fillingham	NSA	dwfilli@missi.ncsc.mil
Richard Guida	Treasury	richard.guida@cio.treas.gov
Michael Jenkins	NSA	mjjenki@missi.ncsc.mil
William Kelly	Treasury	William.Kelly@cio.tras.gov
Gene McDowell	NOAA	emcdowell@iso.noaa.gov
Joseph Mettle	Treasury	Joseph.Mettle@cio.treas.gov
Tim Polk	NIST	wpolk@nist.gov
John Purcell	Treasury	John.Purcell@FMS.sprint.com
Marion A. Royal	GSA	marion.royal@gsa.gov
Shauna Russell	DoD	russells@osdgc.osd.mil
Denise Silverberg	Treasury	Denise.Silverberg@cio.treas.gov
Judith Spencer	GSA	judith.spencer@gsa.gov
Johnny Sumners	Treasury	Johnny.Sumners@cio.treas.gov
Shahira Tadross	DOJ/EOUSA	Shahira.Tadross@usdoj.gov